Efficient Fully Homomorphic Encryption and Digital Signatures Secure from Standard Assumptions(Abstract_要旨)

AUTHOR(S):

Hiromasa, Ryo

CITATION:

Hiromasa, Ryo. Efficient Fully Homomorphic Encryption and Digital Signatures Secure from Standard Assumptions. 京都大学, 2017, 博士(情報学)

ISSUE DATE:

2017-03-23

URL:

https://doi.org/10.14989/doctor.k20511

（続紙１）

京都大学	博士（情報学）	氏名	廣政　良
論文題目	Efficient Fully Homomorphic Encryption and Digital Signatures Secure from Standard Assumptions （標準仮定の下で安全で効率的な完全準同型暗号とディジタル署名）		

（論文内容の要旨）

暗号の研究で最も意義のあることは，重要な暗号機能をいかに効率的に実現するか（いかに実用性の高いものを作るか）ということと，実現した暗号が安全であるということを理論的に証明することである．

本論文では，現在最も重要な暗号機能である高機能暗号（公開鍵暗号が発展・高度化したもので，その代表例が完全準同型暗号）と，認証（ディジタル署名と，それに匿名性を付加したブラインド署名）について，効率性（実用性）と理論的な安全性を兼ね備えた方式を実現するための研究を行っている．本論文で提案する暗号方式は，幅広く用いられており信頼性の高い，標準的な計算量的仮定を安全性の根拠としており（暗号の安全性は何らかの計算量的仮定の下で証明され，最も望ましい仮定は「標準仮定」である），同等の安全性を持つ暗号方式の中では最も効率の良い方式である．

本論文は，全６章からなる．

第１章では序論として，暗号理論とはどのような研究で，そこでは何を目指して研究が行われているのかを概説している．特に，暗号理論においては，重要な暗号機能を効率的に実現することと，暗号機能を実現する暗号方式の安全性を理論的に証明することが重要であることを述べている．また，過去の文献を引用しつつ，本論文で構成された暗号方式（完全準同型暗号，ディジタル署名，ブラインド署名）が重要な暗号機能を効率的に実現しており，標準仮定と呼ばれる暗号理論の研究において確立された計算量的仮定の下で安全性が証明されていることを述べている．

第２章では，本論文を構成する上で基礎となる，暗号理論における安全性証明について概説している．暗号方式の安全性はどのようにして証明されるのか，安全性を保証する計算量的仮定はどのようなに分類されるのか，そして，安全性を証明する際に用いられる数理的モデルについて述べている．

第３章では，高機能暗号の代表例である完全準同型暗号についての研究成果を述べている．完全準同型暗号は暗号化されたままデータを計算できる暗号方式である．例えば，クラウドなどの外部サーバに計算を安全に委託する情報システムにおいて，非常に有用である．特に，本論文で提案する完全準同型暗号方式は，SIMD 完全準同型暗号と呼ばれる，複数のデータを一つの暗号文にまとめて暗号化することができ，暗号化された複数のデータに対して同時に演算を適用することができる完全準同型暗号である．提案する SIMD 完全準同型暗号は，LWE 仮定と呼ばれる標準仮定の下で安

全性が証明されており，同じ仮定を安全性の根拠とする完全準同型暗号よりもシンプルかつ効率的な準同型演算アルゴリズムを持つ．また，提案する SIMD 完全準同型暗号は，Bootstrapping とよばれるノイズ処理アルゴリズムの効率化にも応用できることを示している．

第４章は，認証機能を実現する暗号方式の代表例であるディジタル署名の構成について述べている．ディジタル証明は，受信データが送信元から送られてきたデータであるかということと，受信データが改ざんされていないことを確認する方法を提供する暗号方式である．本章で提案するディジタル署名方式は，RSA 仮定という現在最も幅広く用いられている信頼性の高い標準仮定の下で安全で，同等に安全な他の署名方式よりも，シンプルなアルゴリズムを持つ．また，提案するディジタル署名方式の安全性はランダムオラクルモデルと呼ばれる，現実世界とはかけ離れた数理的モデルの下で証明されている．ランダムオラクルモデルにおいて安全な暗号方式の中には，安全な実装が存在しない暗号方式も知られているが，本章では，提案するディジタル署名は安全な実装が存在するディジタル署名であることを証明している．

第５章は，ディジタル署名に匿名性を付与した暗号方式である，ブラインド署名について述べている．ブラインド署名はディジタル署名の一種で，ユーザと署名者の二者によって行われる暗号プロトコルである．ここでは，ユーザは自身のデータを秘匿したまま署名者に署名を付与してもらうことができる．例えば，電子投票システムにおいて，システムに投票データを秘匿したまま，署名を生成させることができる．提案方式は，既存方式と比較して最も効率の良い方式に匹敵する効率性を持ち，RSA 仮定を安全性の根拠とする初めてのブラインド署名方式である．また，提案ブラインド署名は，第４章で提案されている署名方式と同様に，現実世界において安全な実装を持つブラインド署名であることも証明している．

最後に，第６章は結論であり，研究の背景，目的を踏まえた上で，本論文で示された暗号方式が効率的に重要な暗号機能を実現し，かつその安全性は標準仮定の下で理論的に保証されていることについて述べている．また，今後の展望として，本論文で構成された各暗号方式が社会に対してどのようなインパクトを及ぼすのかを述べている．

注）論文内容の要旨と論文審査の結果の要旨は１頁を３８字×３６行で作成し、合わせて、３，０００字を標準とすること。

論文内容の要旨を英語で記入する場合は、４００～１，１００words で作成し、審査結果の要旨は日本語５００～２，０００字程度で作成すること。

（続紙２）

（論文審査の結果の要旨）

暗号を昨今のネットワーク社会を支える情報セキュリティの基盤技術とするためには，暗号方式が重要な暗号機能を効率的に実現しており，その方式の安全性が理論的に証明されていることが重要である．

本論文は，今日，最も重要な暗号機能とされている高機能暗号と認証について，効率性と理論的な安全性を兼ね備えた暗号方式を実現することを目標に研究を行ったものである．

本論文で提案されている暗号方式は,最も望ましいと考えられている標準仮定を安全性の根拠としており,同等の安全性を持つ暗号方式の中では最も効率の良い方式である．これら一連の研究は，ネットワーク社会において最も重要である情報セキュリティ技術の基盤を確立することに寄与する．

各論で述べられた研究成果は，高機能暗号や認証といった，実社会において重要な暗号機能を効率的かつ安全に実現しており，どれも重要な成果である．第３章では，昨今普及が進んでいるクラウドサービスにおいて有用な完全準同型暗号を，LWE 仮定と呼ばれる標準仮定の下で安全かつ効率的に実現している．第４章においては，ネットワーク社会における攻撃者の代表的な攻撃であるデータの改ざんやなりすましを防ぐ暗号機能であるディジタル署名を，RSA 仮定と呼ばれる標準仮定の下で安全かつ効率的に実現している．また，第５章では，電子投票などの，データを秘匿したまま署名を付与してもらう必要のある場面で有用なブラインド署名を，RSA 仮定の下で効率的に実現する方法を述べている．このように，本論文で述べられている研究成果はどれも，重要な暗号機能を効率的に実現しており，かつ標準仮定と呼ばれる，暗号理論の研究において確立された計算量的仮定の下で安全性が証明されていることから，将来の情報セキュリティ基盤を築くことに寄与する成果であると認められる．

本論文の研究成果は，実社会におけるサイバー攻撃の被害の軽減に資するもので，学術上，実用上寄与するところが少なくない．よって，本論文は博士（情報学）の学位論文として価値のあるものと認める．また，平成２９年２月１５日，論文内容とそれに関連した口頭試問を行った結果，合格と認めた．